Rachel J Hinrichs. Perceptions and Knowledge of Privacy Risks in Mobile Apps. A Master's Paper for the M.S. in L.S degree. April, 2016. 43 pages. Advisor: Brad Hemminger

Consumers often have little knowledge about the extent of privacy risks taken when using mobile applications (apps) on their smartphones, and are unlikely to be informed by federal regulations or privacy certifications. A survey was distributed to smartphone users to determine their perceptions and knowledge of privacy risks in mobile apps, and if these perceptions vary in different contexts (i.e., a health app vs. flashlight app). This study found that people appear to see privacy in mobile apps as contingent and context-dependent. While smartphone users were found to have a good understanding of privacy risks, they considered user rating and price to be more important factors to consider than privacy when selecting a mobile app. Presentation, clarity, and context all influence people's decisions to install and use mobile apps. This study has important implications for how privacy permissions and ratings can be presented to best inform consumer decisions.

Headings:

Privacy

Cellular phones

Disclosure of information

PERCEPTIONS AND KNOWLEDGE OF PRIVACY RISKS IN MOBILE APPS

by
Rachel J. Hinrichs

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Library Science.

Chapel Hill, North Carolina

April 2016

Approved by

_____

Brad Hemminger

Table of Contents

Table of Figures

Introduction

In the last decade, the use of mobile technology has grown at an incredible rate. The rapid adoption of mobile phones, especially smartphones, by consumers created a new market for mobile applications (mobile apps). Mobile apps often combine smartphone capabilities for accessing global positioning systems (GPS) and networks such as 3G and 34 to create interfaces for social networks sites, news feeds, games, health trackers, and even banking. As a result, mobile apps combine all kinds of personal information, some highly sensitive, into one device.

Because mobile apps are useful and convenient, consumers often install and use them with little regard for privacy risks. Mass data collection has become part of everyday life as people rely on the mobile technology for monitoring, storing, and distributing data (Shklovski, Mainwaring, Skúladóttir, & Borgthorsson, 2014). Mobile devices can automatically collect and distribute users' location, personal information, and behavior in real-time. These privacy threats are different than online privacy threats, and potentially more serious (Xu, Gupta, Rosson, & Carroll, 2012). For example, pictures and social media posts can reveal social relationships; geographical data can reveal current and past locations; and accelerometer data can be used to identify the user's current activities.

Efforts by federal agencies and private sector organizations in the United States to regulate mobile apps or set certification standards are limited, and are mostly related to

mobile health apps. The Food and Drug Administration (FDA) has the authority to regulate "medical devices" (Furberg, 2013). Only mobile apps that meet the FDA's definition of a medical device fall under the FDA's jurisdiction, and, even then, the regulation of medical device apps is primarily for safety and effectiveness purposes (Furberg, 2013). Private organizations like Happtique developed standards for mobile health apps that include operability, privacy, security, and content (Misra, 2014). In 2014, however, they experienced a setback when security flaws were found in a number of their certified mobile apps (Misra, 2014). The certification process was also very lengthy and complicated; the company had only been able to certify 70 mobile apps after one year. Because the mobile app market is relatively cheap and easy to enter, it is difficult, if not impossible, for federal agencies and certification companies to keep up with the volume of mobile apps available.

For now, consumers will need to make their own decisions in a "buyer beware" market. Information privacy research can help explain some consumer behavior in selecting and using mobile apps despite their privacy risks. Information privacy research is not new, but has largely changed with the growth of new technologies, especially mobile-based ones (Smith, Dinev, & Xu, 2011). The research in this area is preliminary, and is mostly found in conference proceedings. This study will add to this area of research by examining people's knowledge and perceptions of privacy risks in mobile apps. In particular, this study will determine if people have different privacy risk concerns in different contexts, and how they negotiate privacy risks when selecting apps and allowing privacy permissions. The specific research questions are:

R1. How does selection of a mobile app differ when the privacy rating, user rating, and price are altered? Which of these factors is considered most important when selecting an app?

R2. How do people negotiate privacy risks when allowing privacy permissions, and do their choices vary in different contexts (i.e., a complex vs. simple app)?

R3. What level of knowledge of mobile app privacy risks do adults who own smartphones have?

R4. Does age, gender, type of smartphone, and level of experience affect privacy risk knowledge?

Literature Review

This literature review will describe 1) several of the most predominant theories in information privacy in relation in mobile apps; 2) common privacy risks and issues in mobile apps; 3) consumers' attitudes and perceptions regarding mobile apps and privacy; and 4) researchers' methods for raising user awareness of privacy risks and influencing decision-making.

Information Privacy Theories

Privacy Calculus. One of the most prevalent theories about information privacy and disclosure is privacy calculus, or the notion of privacy as a commodity (Keith, Babb, & Lowry, 2014; Smith et al., 2011). According to this theory, disclosing information is considered a trade-off between benefits and costs. This tradeoff can create a privacy paradox where people claim they have high levels of privacy concerns, but still release private information in many circumstances (Smith et al., 2011). A person's concept of privacy changes depending on the benefits he or she expects to receive. For example, some people may be willing to enter personal health information in order to use a food and nutrition tracker, which they see as highly beneficial. Norberg and colleagues found that for all types of information, including financial, personal identification, and preferences, actual disclosure of information exceeded the individual's' intentions (Norberg, Horne, & Horne, 2007). Another study found evidence of a privacy calculus in

their nationally representative survey of U.S. and Japanese smartphone users (n=1114 U.S. participants and n=2000 Japanese participants) (Fife & Orjuela, 2012). Their results suggest that people are generally not aware that their data are collected or sold to a third party; instead, their actions are influenced by habits, expectations, and cultural practices.

Other researchers have expanded the idea of a privacy paradox to include personalization. When using a mobile device, one of the benefits that users consider is personalization. Personalization can potentially make the experience of using a mobile device more gratifying by delivering individualized services (Sutanto, Palme, Tan, & Phang, 2013). In order to reap the benefits of individualized services, users may forfeit their privacy. In a study comparing a non-personalized mobile app to a personalized one, Sutano and colleagues found that participants used the personalized one more, but their satisfaction was undermined by increased privacy concerns (Sutanto, 2013). Interestingly, their dissatisfaction with privacy concerns was not enough to overcome the benefits of using the personalized mobile app.

Two limitations of the privacy calculus are that it does not account for risks and benefits over time or bounded rationality. Individuals often have limited information, time, and knowledge when making decisions about privacy (Acquisti & Grossklags, 2005). Given a greater knowledge of the risks, or the time to consider them, users may behave differently. Further, information disclosure decisions can change over time. Individuals may discount future risk for present benefits, but become more concerned with privacy risk once the benefit has been achieved (Keith et al., 2014).

Prospect Theory. Privacy calculus can often predict information disclosure intentions, but it does not predict actual behavior, especially future behavior, as well.

Prospect theory can better account for privacy-related behavior over time. Instead of considering risks and benefits at that moment, individuals consider reference points when making decisions (Keith et al., 2014). For example, if the benefits of disclosing information are increasing over time, the individual is in a "gain" position from their original reference point, and will become more risk averse. On the other side, if the benefits of information disclosure are decreasing over time, the individual is in a "loss" position, and will be willing to disclose more information to get back to the original reference point. This theory was supported in Keith and colleagues' longitudinal study of information privacy on mobile devices. In contrast to most studies on privacy risks, this study calculated user's actual behaviors versus their intentions by having participants use a mobile app for 12 weeks. They found that the participants' behavior followed prospect theory more closely than privacy calculus theory. This means that participants became more risk adverse in a gain position, and less risk adverse in a loss position. Though this is the only mobile app privacy study done based on prospect theory, the use of actual behavior versus intended behavior gives it a strong research design that other studies should follow if possible.

Contextual Integrity Theory. While the above theories are concerned with how people choose to disclose information, Helen Nissenbaum's theory of contextual integrity considers context-dependent information flows and social norms (Nissenbaum, 2010). In other words, in different contexts people have different privacy expectations, or, as Nissenbaum describes them, personal information flows. What constitutes personal information in one context may be different in another. In terms of mobile devices and apps, people use apps in a variety of different contexts. Certain privacy risks may be

considered appropriate for some mobile apps (location sharing in a GPS app), but not in others (location sharing in a dictionary app).

A couple of studies examine context and privacy in terms of mobile apps (Lin et al., 2012; Shklovski et al., 2014). Shklovski's study investigated attitudes towards data leakage and tracking on smartphones in different contexts through interviews (n=13), and a survey (n=187) (Shklovski et al., 2014). He made several findings, including that people's expectations of appropriate tracking and data gathering varied between different types of apps. The notion of "creepiness" that many participants described in their interviews was due to the realization that the apps were more than they seemed, and were acting in ways the participants did not agree to or expect. Lin and colleagues had similar findings in their study of privacy expectations and purposes (Lin et al., 2012). Using crowdsourcing on Amazon Mechanical Turk, they had the particpants check off what type of privacy permissions they would consider reasonable for various types of mobile apps. Like in Shklovski's study, participants were highly concerned when mobile apps collected information they did not expect; however, Lin and colleagues found that if users were informed why a given data was being used, their privacy concerns could be allayed to some extent.

Common Privacy Risks in Mobile Apps

Before analyzing people's perceptions of apps, it is useful to first see what privacy risks are prevalent in mobile apps, and how are they presented to consumers in the app itself or in its description in the app store. Most of these studies focus specifically on health-related mobile apps or location-based apps due to their clearly personal nature.

One approach to studying privacy issues in mobile apps is analyzing the content of privacy policies. Sunyaev and colleagues assessed the availability, scope, and transparency of health-related mobile app privacy policies (Sunyaev, Dehling, Taylor, & Mandl, 2014). Of the 600 most popular apps on the iOS and Android stores, only 30.5% had privacy policies, and these policies were very long and written at a college reading level (Sunyaev et al., 2014). If users wanted to read the privacy policies, which may not be likely, the policies may be too difficult to understand or not even available. A report from the Privacy Rights Clearinghouse analyzed the privacy policies, permissions required, and content of 43 popular health and fitness apps, both paid and free (Ackerman, 2013). They found that 26% of free apps and 40% of paid apps had no privacy policy, and that less than 50% of apps notify users of information they make public or send to third-parties (Ackerman, 2013). Note that this report may have inherent bias due to the authors' affiliation; however, their analysis started with no knowledge of the mobile apps selected, and the evaluation was carefully documented and made available on their website. Mobile app privacy policies are not easily accessible to consumers either because they do not exist or because they are written and presented in a way that no one would read them.

Researchers have also used technical analysis of data practices of mobile apps. Several studies had users install an app that would track personal data flow. One showed that access to address book information is the biggest concern, and that over half of the connections made by apps are insecure (Ferreira, Kostakos, Beresford, Lindqvist, & Dey, 2015). The other study found that the majority of application network data is sent to advertisement servers without user consent or knowledge (Enck et al., 2014). In another

study, Fu and colleagues found that user location data is frequently sent without the user's consent or understanding of the reasons for it (Fu, Yang, Shingte, Lindqvist, & Gruteser, 2014). The Privacy Rights Clearinghouse also did a technical analysis, and found that only 10-13% of apps encrypt all connections to the developer, and that about a third of apps tested sent data to a party not covered in the privacy policy (Ackerman, 2013). These studies reveal that privacy risks are fairly extensive, and are most related to personal information and location services.

Consumer Attitudes and Preferences towards Privacy Risks in Mobile Apps

Many studies have sought to find out how much consumers know about privacy risks, and what their perceptions of privacy risks in mobile apps are. These studies have used a variety of primarily qualitative methods, including surveys, interviews, observations, and focus groups, and have identified several themes.

First, as per Nissenbaum's contextual integrity theory, Atienza and colleagues have found that consumer attitudes are highly contextualized and more nuanced than the privacy paradox suggests (Atienza et al., 2015). In their study of 24 focus groups with 256 participants, Atienza and colleagues found that participants' concerns about privacy depended on the type of information, where and when the information is accessed, and who is seeing the data. Control was an important issue. Many participants were willing to reveal personal information in order to reap the benefits of personalization and usefulness, but wanted to control when and where this happened.

Several studies show that privacy concerns vary by age, degree of use, and risk knowledge. One study found that the degree of concern about privacy and security issues increased as age increased (Fife & Orjuela, 2012). They suggested that this could be

because older adults tend to have less experience with mobile devices. A study of African American young adults found that the participants were not generally concerned about privacy (Park & Jang, 2014). The young adults were generally unaware of data leakage or third party advertisers, and referred instead to interpersonal privacy concerns such as locking their phone so a family member could not access it. Perceived skill level also appears to influence privacy concerns. As consumers' perceived skill level increases, they seem less concerned with privacy, perhaps due to increased use of mobile devices, or confidence in their ability to control the situation (Keith, Thompson, Hale, Lowry, & Greer, 2013). Another study by Pew Research, however, found no consistent demographic answers by age, income, education, or gender when participants were asked about their opinions on data sharing in various contexts (Rainie, et. al., 2016). Consumer attitudes toward privacy are overall nuanced, contextual, and possibly related to age, skills, and degree of use.

Methods for influencing or informing consumers' decisions about privacy

Because many consumers have little knowledge of privacy risks and are unlikely to be informed by federal regulations or mobile app certification programs, researchers have been developing methods for influencing or informing consumers' decisions when selecting mobile apps. Android currently has a permission system that is intended to inform users about the privacy risks involved with certain mobile apps. Before installing an app, the consumer can review the permission requests, and cancel the installation if it seems excessive. While this permission system is an important step in providing privacy information to consumers, Felt and colleagues in their study of 308 Android users found that users had low comprehension of the Android permissions and paid little attention to

it (Felt et al., 2012). They concluded that these warnings do not help users make privacy decisions.

Some studies have modified the Android permission display, or created a new one, to see if it would play a more active role in app selection. The first study modified the Android permissions display into a simplified privacy checklist that fits on the main app description screen (Kelley, Cranor, & Sadeh, 2013). The location of the checklist is important because consumers may have already made their decision regardless of the privacy permissions if they have already clicked install. In this way, the checklist may be more likely to influence consumer decisions. Kelley and colleagues found in both a lab study and a large-scale online survey that users noticed the new display, and that it affected their selection decisions, especially when deciding between similar apps (Kelley et al., 2013). Another couple of studies designed new privacy indicators based on warning design theory (Bal, 2014) and visual framing effects (Choe, Jung, Lee, & Fisher, 2013). Both found that the visual representation of privacy risk quickly and effectively informed consumers of the risks involved, and influenced their decisions to some extent. Representing privacy risks visually and in a simplified manner before installation appears to help inform consumers of privacy risks, and may influence their final decision.

Literature Review Summary

Based on the studies above, consumers appear to make cost-benefit decisions based on the specific context when it comes to privacy. Many consumers also have little knowledge about the extent of the privacy risks taken when using mobile apps. Further, they are unlikely to be informed by federal regulations or privacy certifications because the amount of apps available is enormous and grows every day. Visual representation of

degree of privacy risk appears to help inform and influence consumers' decisions. However, it is unknown whether these would have an effect in a "real-life" scenario where consumers are also considering factors such as user reviews and cost. In conducting this literature review, there appears to be a need to determine how people negotiate privacy risks when selecting apps and allowing privacy permissions in different contexts, and whether privacy risk knowledge and demographic factors correlate with these choices.

Methods

The following section will describe the methods, population, sampling, data collection, and plans for analysis of this study.

Selection of Method

This study will use a self-administered, web-based survey to gather data. A survey is ideal for this type of research for several reasons. One, surveys are designed so that only small percentage of the population is needed to draw conclusions about the larger population (Wildemuth, 2009). This means less time and resources are required to gather data. Two, surveys can allow the researcher to analyze several variables at one time. This study will analyze several variables, including age, privacy rating, user rating, price, privacy permissions, and privacy risk knowledge. The questions in this survey will also be close-ended making this analysis easier. Third, web-based surveys can be distributed widely and cheaply, which could potentially increase the diversity of the sample. This would also allow more subgroups to be represented in the analysis, for example those with a high versus low privacy risk knowledge.

Population & Sampling

The population of interest is adults (18 years and older) who own or use a smartphone. This population is purposely broad to enable the identification of subgroups. The most important requirement is that the population uses a smartphone, otherwise they may not be familiar with mobile apps.

A convenience sample was taken by distributing the Qualtrics survey link via an email message to university mailing listservs that include undergraduate and post-graduate students, faculty, and staff. It was also distributed via the investigator's social networks on Facebook and Twitter. Snowball sampling was also used because the investigator's friends and family forwarded the link to their contacts. The survey was open for a three-week period during which the participants could click on the link and submit their responses via Qualtrics. While a convenience sample is not ideal for representative sampling, it was sent to different mailing listservs and groups that include individuals of different ages and in different locations to attempt to diversify the sample.

In order to encourage participation, participants were offered the chance to enter a drawing for one of four $50 Amazon gift cards. Funding for this incentive was provided by a Carnegie Grant through the School of Information and Library Science at the University of North Carolina at Chapel Hill. After completing the questionnaire, participants had the option to enter their email address. Email addresses were exported to a spreadsheet, and four were selected using a random number generator. These gift cards were distributed in March 2016.

Survey Content

The survey consisted of four sections.

Section 1: Demographics. This section first confirmed that the participant is over the age of 18 and owns a smartphone, which are both requirements to take this survey. Then the participant was asked basic demographic questions such as age, gender, and student type (if they are a student). It also asked how long the person has owned a smartphone and the platform they use.

Section 2: Mobile app selection. This section seeks to answer R1: How does selection of a mobile app differ when the privacy rating, user rating, and price are altered? Which of these factors is considered most important when selecting an app? Mobile app stores typically display a price and a user rating on a 5-point scale for each app. This section will display both the price and user rating, but also add a privacy rating on a 5-point scale, with 1 being a poor privacy rating (i.e., lack of security) and 5 being an excellent privacy rating (i.e., high security). The privacy rating is included to test how it affects the participants' selection of a mobile relative to the user rating and price. Because this section deals with user perceptions of privacy risks as a component of the decision-making process when selecting apps, it was placed first in the survey (after the demographics) to prevent bias. If it was placed later in the survey, the participants will likely realize the survey is about privacy, which may affect their responses.

This section was based on the survey done by Choe and colleagues (Choe et al., 2013). Their study tested whether presenting positively- and negatively-framed privacy rating scales with or without a user rating of 3 affected the participants' selection of a mobile app. This survey built on their design by incorporating price and varying the user and privacy rating scores to a greater extent. The goal was to find a threshold where participants balanced the perceived privacy risks with the user rating and price. A pilot test helped to determine which combinations of privacy and user ratings and price were the most appropriate. In order to rank the factors in order of importance to the participants, each combination of privacy rating, user rating, and price will be sorted according to the survey results and transitive logic.

Section 3: Privacy Permission Selection. This section focuses on R2: How do people negotiate privacy risks when selecting or allowing privacy permissions, and do their choices vary in different contexts (i.e., a complex vs. simple app)? There are many different types of privacy permissions for mobile apps, and participants may feel some are more important to them than others. For example, some participants may want to turn off location-finding services, but will let the app access their contact information. Further, participants may believe some privacy permissions are appropriate in certain types of apps, but not in others.

Because appropriate permission settings may be perceived differently in various contexts, three different apps were briefly described to the participants:

1. FoodWise: Track your diet and exercise, and easily connect to other devices, such as Fitbit, or to your selected contacts to motivate each other. Receive personalized goals based on your diet profile, or enter your own goals based on advice from your doctor or dietitian.

2. Bright Light: This app instantly turns your phone into a flashlight. Now with an easy-to-use interface and strobe mode.

3. Navigator: This GPS app will find routes, restaurants, shopping, friends, and more!

Participants were then given a list of data types that the app could collect. For each data type, they indicated whether they would, would not, or would maybe allow the data to be collected. Participants were reminded that limiting data access might affect the functionality of the mobile app.

Figure 1. Data types for the privacy permission selection

Data Types
Contact information
Location-sharing
Photos/camera
Audio/microphone
Contacts list
Social media – Facebook
Social media – Twitter
Medical information – Physical (height, weight, gender)
Medical information – Diagnoses (diabetes, asthma, food allergies)

Section 4: Privacy Risk Knowledge. This section focuses on R3: What level of knowledge of mobile app privacy risks do adults who own smartphones have? This section was based off the privacy risk knowledge survey conducted by Parks and colleagues with some question additions and subtractions (Park & Jang, 2014). This section consisted of 8 true/false questions on privacy risks in mobile technology. The sum of correctly answered questions is the user's privacy risk knowledge score.

To answer R4: Does age, gender, type of smartphone, and level of experience affect privacy risk knowledge?, analysis of variance (ANOVA) will used to determine whether there were any significant differences between the variables. If ANOVA shows any significant difference between variables, the Scheffe test will be used to determine between which variables there was significant difference.

Ethics

Survey methods are generally low-risk in that they do not cause physical harm and are unlikely to cause psychological harm. The main ethical concerns for this study are the assurance of privacy and anonymity. No identifying information will be retained. The only personal information gathered was the email addresses of the participant who

wanted to enter the drawing; these email addresses were exported, and then deleted shortly after the drawing was completed.

Because this study deals with human subjects, it was submitted to the University of North Carolina at Chapel Hill's Institutional Review Board (IRB) for review. All study methods, procedures, and materials were approved by IRB in January 2016 before releasing the survey.

Results

Sample Demographics

After the survey was open for 3 weeks, 111 surveys were submitted. Eight surveys were not complete; participants dropped the survey around the start of section 2 (selecting a mobile app) or section 3 (selecting privacy permissions). These surveys were removed. The total of complete surveys was N=103, a completion rate of 93%.

The combination of convenience and snowball sampling gathered a sample that skewed young, female, tech-savvy, and Apple-friendly. Figures 3 and 4 show the age and gender of the participants who completed the test. Seventy-two participants reported that they are students (65% of the total sample); 74% of the students are master's students and 25% are undergraduates**.**

Figure 2. Gender of Participants

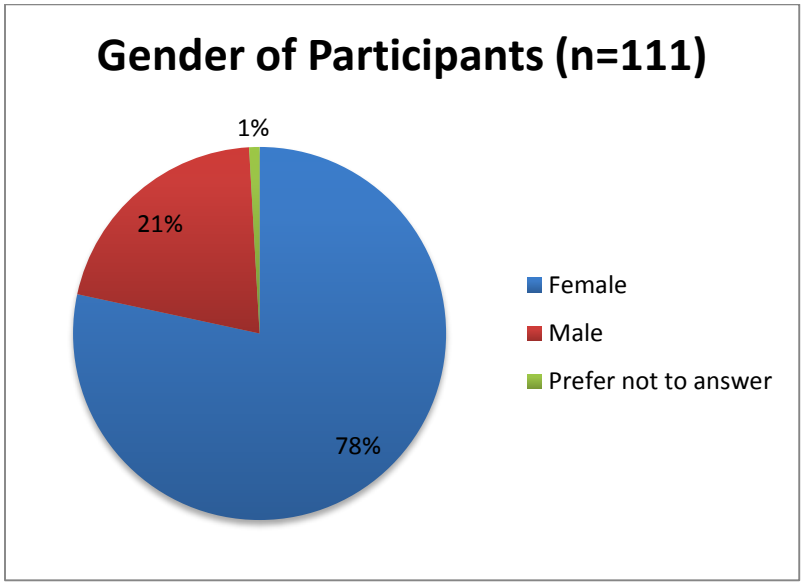
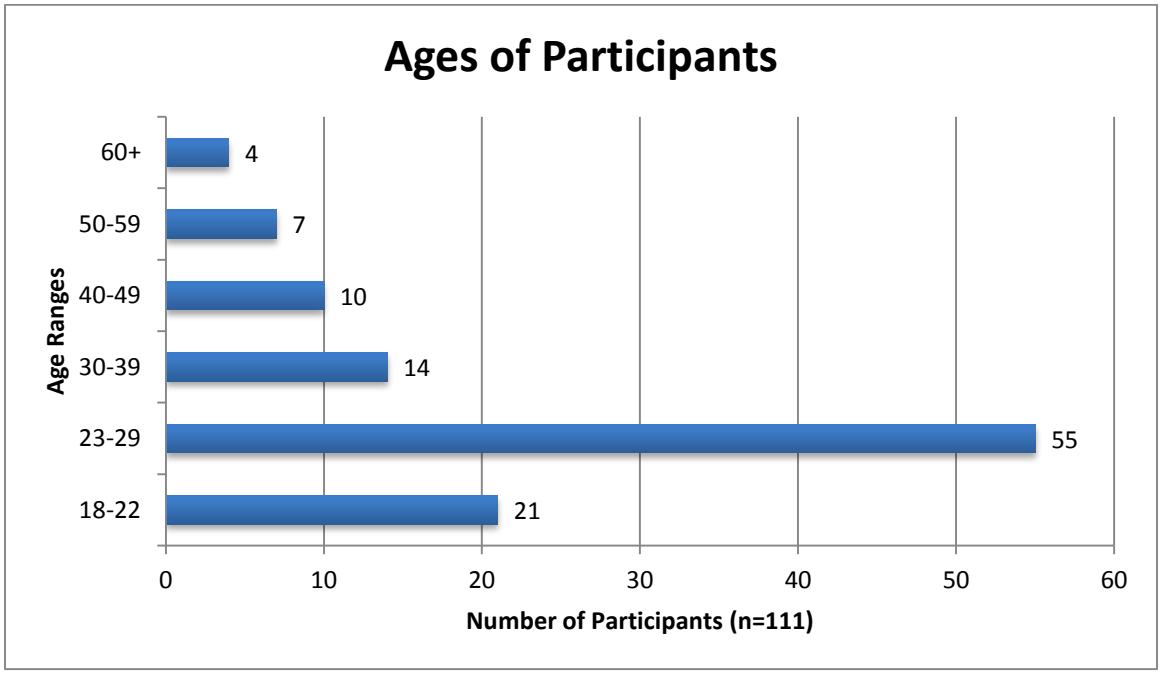


Figure 3. Ages of Participants



Participants were also asked what kind of smartphone they own, and how long they have owned a smartphone. Apple users and tech-savvy individuals were over-represented in this survey likely due to the survey being sent to the School of Information and Library Science email lists. iPhone users were 68% of the responses. By far most participants have owned a smartphone for at least three years, with 38% having owned a smartphone for over 5 years.

Figure 4. Type of Smartphone Owned

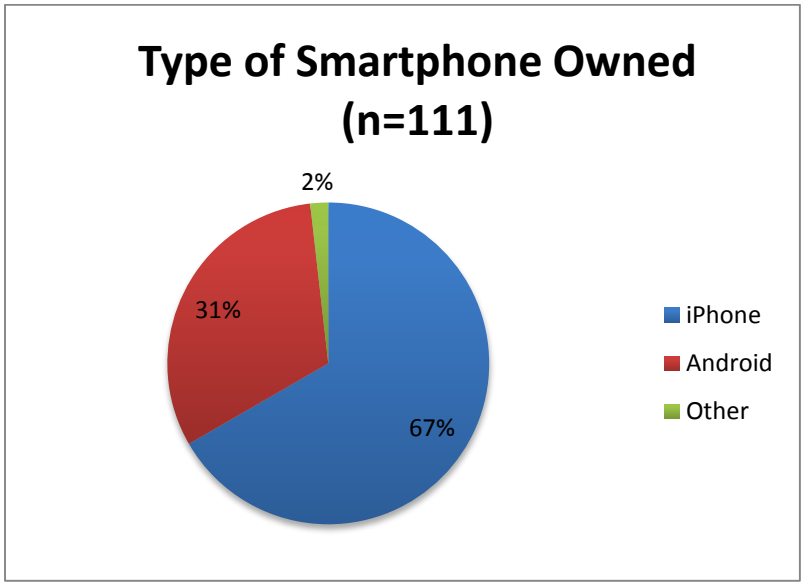
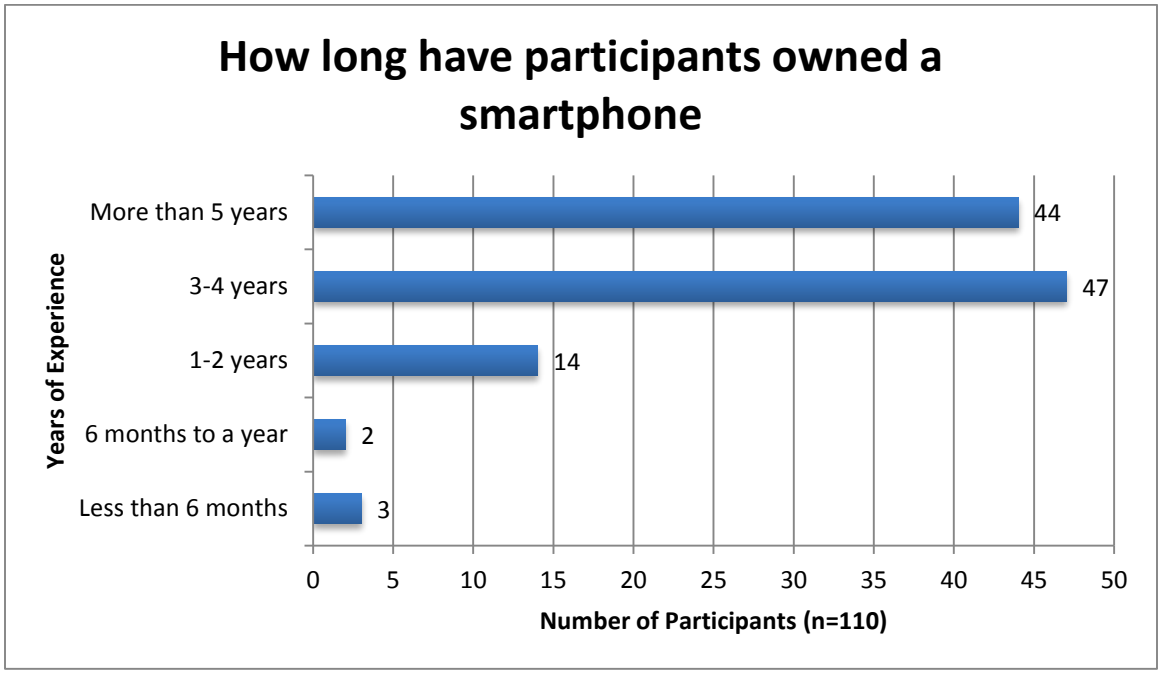


Figure 5. How long have participants owned a smartphone



Mobile App Selection

This section had participants compare two mobile app descriptions that included user and privacy ratings on a 5-point scale, and a price, either free or $.99. These three

factors were varied in order to see how participants negotiate privacy risks with price and user ratings, two of the main criteria people use to select between apps to install.

The first three questions compared apps with varying user and privacy ratings with the price held constant at free. As Figures 4-6 show, about 75% of the participants for each question selected the app with highest user rating over the privacy rating.

Figure 6. Example question

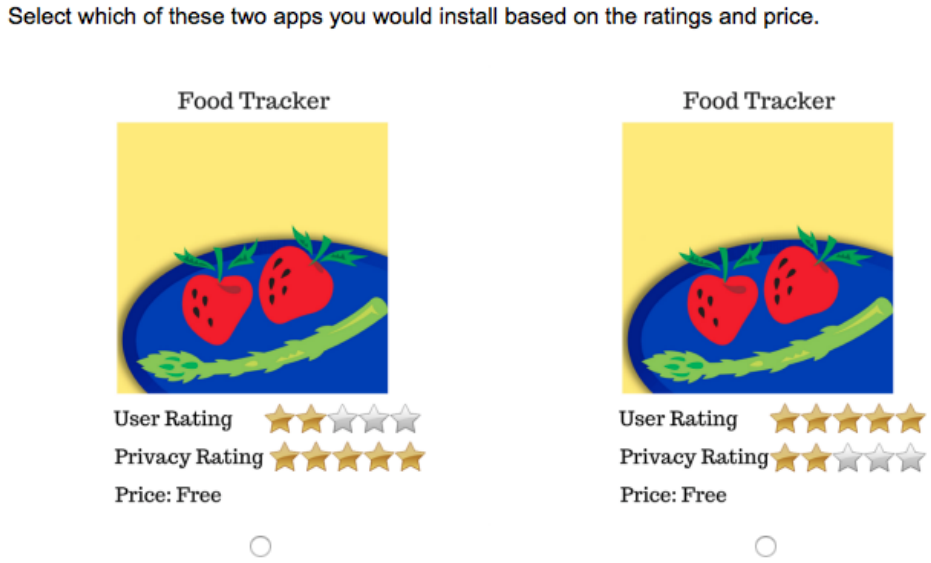


Figure 7. Mobile App Selection 1

Rating Comparison	Number of Responses	Percentage
User Rating ★★☆☆☆ Privacy Rating ★★★★★ Price: Free	27	25%
User Rating ★★★★★ Privacy Rating ★★☆☆☆ Price: Free	83	75%
	110	100%

Figure 8. Mobile App Selection 2

Rating Comparison	Number of Responses	Percentage
User Rating  Privacy Rating  Price: Free	31	28%
User Rating  Privacy Rating  Price: Free	78	72%
	109	100%

Figure 9. Mobile App Selection 3

Rating Comparison	Number of Responses	Percentage
User Rating  Privacy Rating  Price: Free	80	73%
User Rating  Privacy Rating  Price: Free	29	27%
	109	100%

The last two questions compared apps with varying prices and privacy ratings, while the user rating was held constant at 4 stars. 64% of the participants selected the free app with a privacy rating of 3, when compared to the $.99 app with a privacy rating of 5. This percentage, however, dropped to 50% when the privacy rating was 2. In other words, participants were more willing to install a paid app when the privacy rating dropped below 3.

Figure 10. Mobile App Selection 4

Rating Comparison	Number of Responses	Percentage
	39	36%
	70	64%
	109	100%

Figure 11. Mobile App Selection 5

Rating Comparison	Number of Responses	Percentage
	53	50%
	54	50%
	107	100%

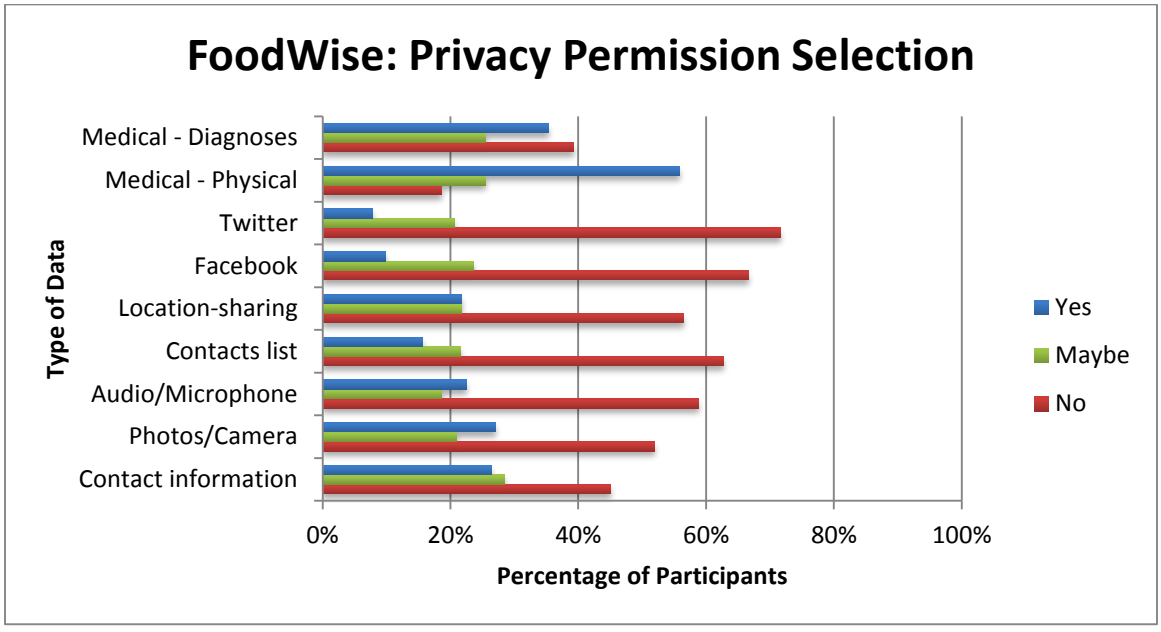
Privacy Permission Selection in Context

This section had participants select which types of data they would or would not allow three mobile apps to access. The mobile apps varied in complexity, from a health and food tracker to a GPS navigator to a flashlight. Over nearly all data categories,

participants indicated that they would not allow the mobile apps to access their data. There were, however, some exceptions based on the type of mobile app.

For FoodWise, the health and food tracker, most participants indicated that they would not allow the app to collect most data with the exception of physical medical information (e.g, height, weight, gender). It may be that participants considered physical medical information a reasonable type of data for this app to collect in order to function properly or to be personalized for their needs. While more participants declined access to diagnoses medical information (e.g., diabetes, asthma, food allergies), the percentage between 'no' and 'yes' was very close (39% versus 35%, respectively), again indicating that many participants were negotiating between the privacy risk and the benefits of making their medical data accessible.

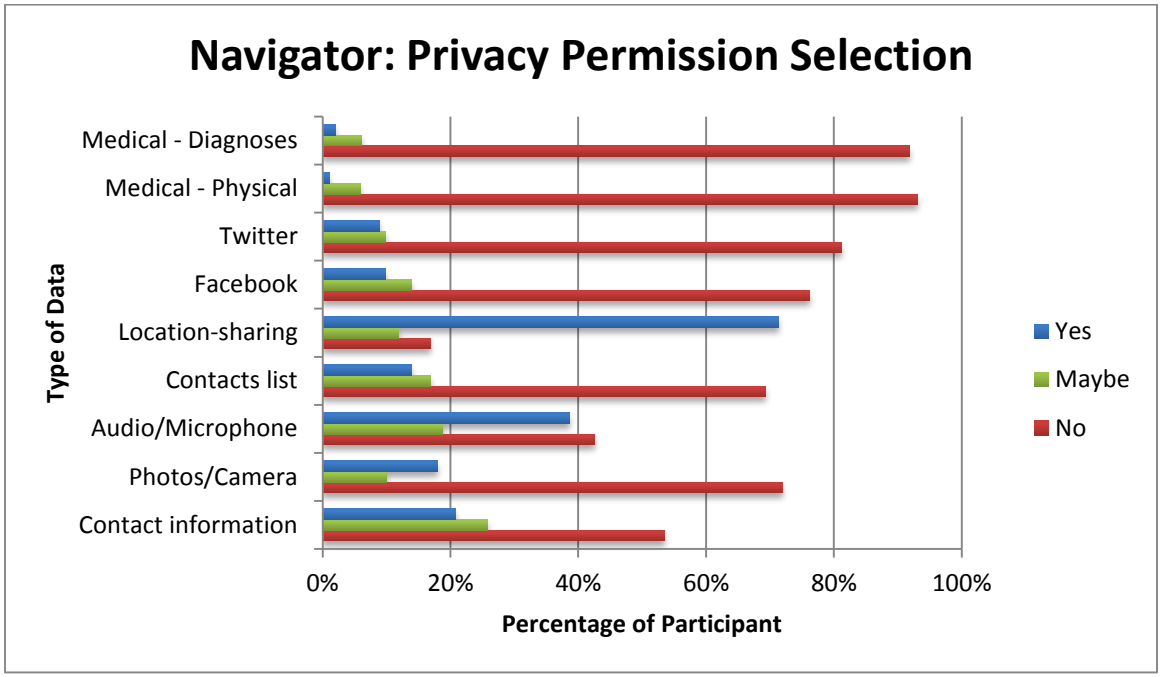
Figure 12. FoodWise: Privacy Permission Selection



Similarly, for the Navigator mobile app that uses GPS, participants were more willing to allow access to their location data with 76% participants selecting 'yes' and

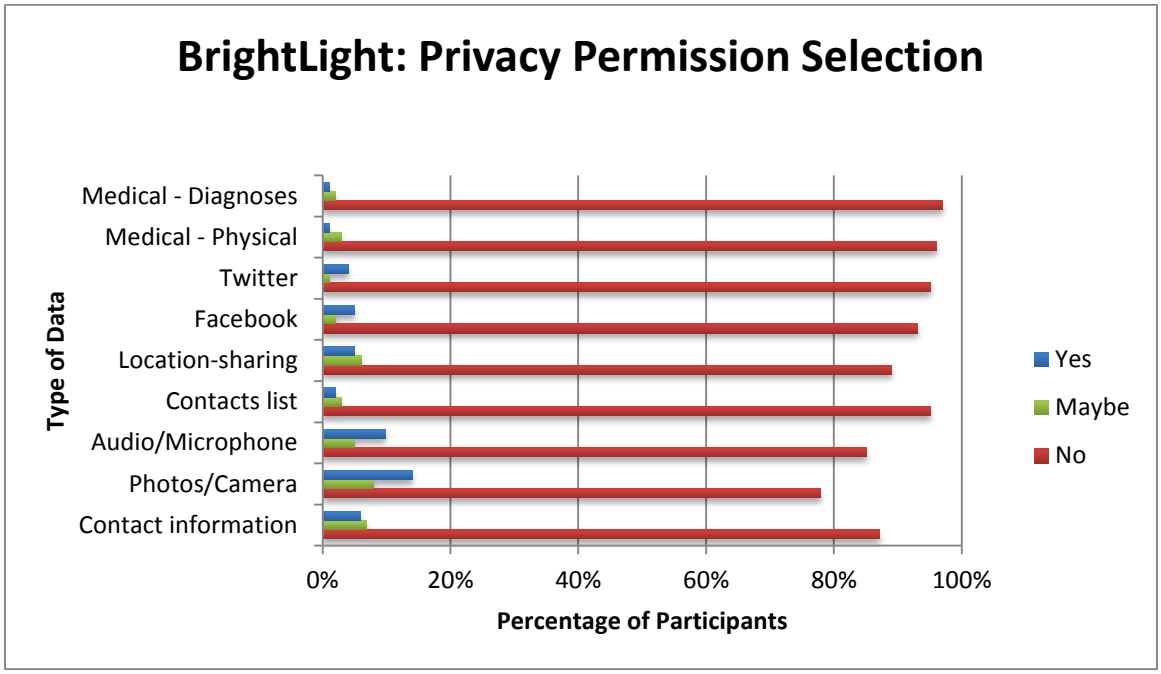
12% selecting ‘maybe.’ Sometimes GPS apps use audio to give directions. Most participants denied access to the audio/microphone at 43%, but those allowing access was very close at 39%.

Figure 13. Navigator: Privacy Permission Selection



By far the majority of participants were opposed to allowing BrightLight, the flashlight app, to access their data. A flashlight app generally only needs access the flash on the camera in order to function, though it is unknown how many participants would know this. There is a slight increase in participants selecting ‘yes’ (14%) and ‘maybe’ (8%) for the photos/camera option, which could indicate that a small percentage of participants were aware of this and were willing to allow the app to access the camera flash. Otherwise, participants were very opposed to allowing a flashlight app collect any data.

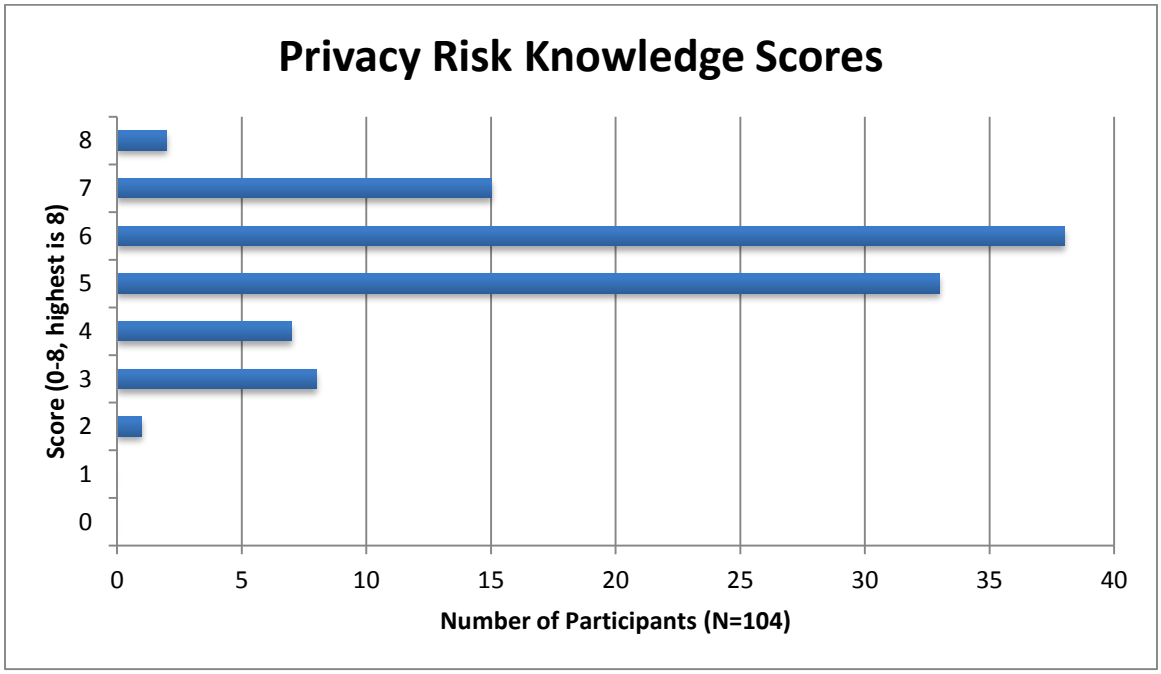
Figure 14. BrightLight: Privacy Permission Selection



Privacy Risk Knowledge

Each participant answered 8 true/false questions on privacy risks related to mobile phones and apps. The privacy risk knowledge score was calculated by adding 1 point for every correct answer and 0 points for every incorrect answer for a high score of 8. The average privacy risk knowledge score was 5.4. Only two participants received perfect scores of 8, and all participants answered at least 2 questions correctly. Figure 15 displays the number of participants who got each score.

Figure 15. Privacy Risk Knowledge Scores



Participants were well aware that companies and social media websites monitor their browsing and use their data for advertising. Most participants answered questions such as "Most mobile apps, such as m-Facebook or m-Yahoo, monitor and record your browsing" correctly (89%). Nearly all participants answered, "Companies today have the ability to place an ad that targets you based on information collected on your mobile phone" correctly (99%). Participants were less certain, however, on more technical questions. 60% of users answered true for the question "The goal of encrypted data transmission is that only the user can see the data," when the answer is false.

ANOVA was used to determine if there are differences in privacy risk knowledge between subgroups. Differences in age, for example, may show that older adults are less or more knowledgeable about privacy risks than adults under 30. Because this sample was skewed to people in their 20s and had much lower amount of participants older than 40, ANOVA was performed twice, once with the original age groups (18-22, 23-29, 30-3,

40-49, 50-59, and 60+), and again with participants in their 40s, 50s, and 60+ grouped together (18-22, 23-29, 30-39, 40+). ANOVA with the original age groups found that there was a significant difference between the groups. ANOVA with the combined older age group did not find a significant difference between the groups. This difference could be because there were very few participants in the 40-49, 50-59, and 60+ age ranges compared to the 18-22 and 22-29 age groups. Combining the 40s, 50s, 60s age groups made a sample closer in size to the 18-22 and 22-29 age groups, but there was no longer any significant difference. A more comparable sample size between age groups could confirm if there is no difference in privacy risk knowledge between different age groups.

Figure 16. ANOVA analysis for original age groups & privacy risk knowledge score

Source of Variation	Sum of Squares	d.f.	Mean Squares	F
between	20.00	5	4.001	3.218
error	121.8	98	1.243	
total	141.8	103		

The probability of this result, assuming the null hypothesis, is 0.0099

Figure 17. ANOVA analysis for combined age groups & privacy risk knowledge score

Source of Variation	Sum of Squares	d.f.	Mean Squares	F
between	7.850	3	2.617	1.953
error	134.0	100	1.340	
total	141.8	103		

The probability of this result, assuming the null hypothesis, is 0.13

ANOVA analysis was also done for level of experience as indicated by the years an individual has owned a smartphone, gender, and type of smartphone. Only gender was found to be statistically significant.

Figure 18. ANOVA analysis for gender & privacy risk knowledge score

Source of Variation	Sum of Squares	d.f.	Mean Squares	F
between	5.984	1	5.984	4.528
error	133.5	101	1.322	
total	139.5	102		

The probability of this result, assuming the null hypothesis, is 0.036

Discussion

R1. How does selection of a mobile app differ when the privacy rating, user rating, and price are altered? What factor is considered the most important to selection of a mobile app?

In order to determine how participants negotiated between privacy rating, user rating, and price, participants' preferences from section 1 were compared and ranked using the transitive property. This process revealed that participants consistently ranked user rating the most important, followed by price, and lastly privacy rating. User rating can be related to the functionality and usability of the app; if an app has a low user rating, about three-quarters of participants are not going to install it, no matter the privacy rating. Price, however, can help mediate this affect. If the user rating is fairly high, once the privacy rating dips below 3 stars, users are willing to pay for a more secure mobile app.

There are some limitations based on the comparison questions asked. It is possible that a threshold exists where privacy and user rating are more balanced. Additional comparisons would need to be asked to determine where the balance point is. Another limitation is that no comparison questions were asked that changed all three factors at the same time. This was done in order to isolate specific changes, but additional questions varying all three factors could help pinpoint nuances in how people negotiate these factors.

Even so, it is clear from the results of this study that user rating is by

far the most important factor considered. Any company or organization wanting to add a privacy rating scale to the app stores may need to consider alternate ways to present the information. Customers may not notice the privacy rating or ignore it depending on what the user rating is.

R2. How do people negotiate privacy risks when selecting or allowing privacy permissions, and do their choices vary in different contexts?

Based on the trends displayed in Figures 12-14, most participants were cautious about allowing the mobile app to access their data except in specific, function-related circumstances. Most participants would allow the food and nutrition tracking mobile app to access their physical medical information; similarly, a strong majority of people would allow the GPS app to track their location. They were very opposed, however, to allowing the flashlight app to access any data. These results align with the Nissenbaum's theory of contextual integrity and Shklovski's study of mobile app "creepiness" (Nissenbaum, 2010; Shklovski et al., 2014). Certain privacy permissions are considered acceptable in certain contexts, but inappropriate in others. A flashlight app that collects data outside of its purpose would likely seem inappropriate and even creepy to many people. What is considered acceptable also varies by person, and what their purpose for using the app is. For example, some individuals may want to use the food and nutrition tracker with social media in order to connect with friends. In this study, 24% of participants would allow this app to access Facebook and 21% would allow it to access Twitter. Other individuals, however, may consider this a major privacy infringement (72% for Twitter and 67% for Facebook).

Some participants are willing to reveal personal information in order to use certain app functions or personalize it to their needs or preferences. Control over where and when this happens is likely to be the main issue. Future research could delve more into this concept by seeing if participants would or would not allow, for example, a GPS app to access their location when they are not using it as opposed to when they are.

R3. What level of knowledge of mobile app privacy risks do adults who own smartphones have?

Based on a short, true/false quiz, the participants of this study were overall knowledgeable about mobile phone and app privacy risks. The average score was 5.4 questions correct out of 8, and the median score was 6. As expected, participants were well aware that companies collect their data and use it for advertising.

Participants were less aware about the more technical aspects of privacy. Most participants (79%) incorrectly answered the question "Most app permissions seek access to a device's hardware, rather than a user's personal information." This may be due to a misconception that privacy risks are only or usually related to accessing personal information. A Pew Research reported that 70% of Android app permissions seek access to the device's hardware, such as Internet connectivity or camera flash, rather than personal information (Anderson, 2015). This is an important distinction to consider when displaying privacy permissions. If individuals generally consider privacy permissions to be related to personal data, they may misunderstand that most mobile apps are asking for hardware-related permissions such as access to the flash or vibrator. Dismissing these permissions will affect the functionality of the mobile app. A short explanation

explaining why an app needs permission for a particular function may help in these circumstances.

R4. How does age, gender, type of smartphone and level of experience relate to privacy risk knowledge?

According to the results of the ANOVA tests, only the participants' gender showed a statistically significant affect on privacy risk knowledge score. On average, women scored 5.3, and men scored 5.9. This effect could be due to the sampling; there were almost four times the number of women (n=81) completing the survey than men (n=21).

For age, a statistically significant effect was found for the original age groupings (18-22, 23-29, 30-39, 40-49, 40-59, 60+). This effect disappeared when the participants who were 40+ years were grouped together to create a more comparable sample size to the younger age groups (18-22, 23-29, 30-39, 40+). With this data, it is difficult to say if there is a statistically significant effect of age on privacy risk knowledge. A broader sample that includes a similar number of older and younger individuals could confirm if this difference is statistically significant. However, these results do align with a study done by Pew Research. When asked about the acceptability of different scenarios on privacy risks, Pew Research found no consistent demographic answers by age, income, education, or gender (Rainie, et. al., 2016).

Limitations

There are several limitations to this research study. First is the sampling method. Convenience and snowball sampling have the advantage of being quick and cost-effective, but they almost inevitably lead to results that are not generalizable to rest of the

population. This sample was primarily collected from university post-graduate students in their 20s. This group may be more knowledge about technology and privacy, and may have different opinions on privacy compared to the rest of the population. Because of this sample representation, it was difficult to use ANOVA analysis to differentiate between sub-groups, especially age or experience. Further, not all individuals who received the email message filled out the survey. It could be that the individuals who answered the survey had different opinions and knowledge about privacy and mobile apps.

A second limitation is that this survey measured the individual's intentions, not their actual behavior. This is a common issue with studies involving mobile technology and privacy, and few studies have been able to devise their methodology to measure actual behavior (Keith et al., 2014). While intentions can tell us much about people's opinions and state of mind regarding privacy, the privacy paradox theory suggests that intentions do not often match with behavior. In the case of this research study, participants may not want the mobile apps to access their data except in specific circumstances, but in the real world would allow it to happen. This could happen because they want to reap the benefits of the app anyway, do not know that the app is collecting the data, or they cannot or do not know how to turn it off.

Lastly, while this survey was designed to gather quantitative data, qualitative data could give more insight into why the participants responded the way they did. Qualitative data might reveal more of the nuances of why participants selected a certain app, or would turn on or off particular privacy permissions.

Conclusion

Mass data collection enabled by the unprecedented growth of smartphones and mobile apps has become part of everyday life. Consumers have little knowledge about the extent of privacy risks taken when using mobile apps, and are unlikely to be informed by federal regulations or privacy certifications. This study examined people's knowledge and perceptions of privacy risks in mobile apps, particularly how they negotiate risks in various contexts. Generally people see user rating as the most important factor to consider, followed by price, both of which give some indication of the usability and usefulness of the mobile app. This study showed that privacy rating was the least important factor people considered when selecting a mobile app. Despite knowledge of privacy risks, most consumers appear to see privacy in mobile apps as contingent and context-dependent. This study has important implications for how privacy permissions and ratings can be presented to consumers to best inform their decisions. Presentation, clarity, and context all influence consumers' decisions to install and use mobile apps. Developers, researchers and policy-makers need to be understand the trade-offs that consumers are willing to make, and explicitly provide consumers with explanations for privacy permissions and options to modify privacy settings. Hopefully in the future, consumers will have the information about privacy and mobile apps needed to make well-informed decisions.

Bibliography

Ackerman, L. (2013). Mobile Health and Fitness Applications and Information Privacy. *Privacy Rights Clearinghouse, San Diego, CA*.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*(1), 26-33.

Anderson, Monica. (2015). Key takeaways on mobile apps and privacy. *Pew Research Center*. Retrieved from: http://www.pewresearch.org/fact-tank/2015/11/10/key-takeaways-mobile-apps/

Atienza, A. A., Zarcadoolas, C., Vaughon, W., Hughes, P., Patel, V., Chou, W. Y. S., & Pritts, J. (2015). Consumer Attitudes and Perceptions on mHealth Privacy and Security: Findings From a Mixed-Methods Study. *Journal of Health Communication, 20*(6), 673-679. doi:10.1080/10810730.2015.1018560

Bal, G. (2014). *Designing privacy indicators for smartphone app markets: A new perspective on the nature of privacy risks of apps.* Paper presented at the 20th Americas Conference on Information Systems, AMCIS 2014.

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing *Human-Computer Interaction–INTERACT 2013* (pp. 74-91): Springer.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., & Sheth, A. N. (2014). TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. *ACM Trans. Comput. Syst., 32*(2), 1-29. doi:10.1145/2619091

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). *Android permissions: user attention, comprehension, and behavior*. Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, D.C. http://dl.acm.org/citation.cfm?doid=2335356.2335360

Ferreira, D., Kostakos, V., Beresford, A. R., Lindqvist, J., & Dey, A. K. (2015). *Securacy: an empirical investigation of Android applications' network usage, privacy and security*. Paper presented at the Proceedings of the 8th ACM

Conference on Security & Privacy in Wireless and Mobile Networks, New York, New York. http://dl.acm.org/citation.cfm?doid=2766498.2766506

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management, 5*(6), 7.

Fu, H., Yang, Y., Shingte, N., Lindqvist, J., & Gruteser, M. (2014). A field study of run-time location access disclosures on android smartphones. *Proc. USEC, 14*.

Furberg, R. (2013). The regulatory context of mobile health in the United States and a conceptual framework for privacy and security. *European Journal of ePractice, 21*, 66-75.

Keith, M. J., Babb, J. S., & Lowry, P. B. (2014, 6-9 Jan. 2014). *A Longitudinal Study of Information Privacy on Mobile Devices.* Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies, 71*(12), 1163-1173. doi:10.1016/j.ijhcs.2013.08.016

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). *Privacy as part of the app decision-making process.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). *Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing*. Paper presented at the Proceedings of the 2012 ACM Conference on Ubiquitous Computing, Pittsburgh, Pennsylvania.

Misra, S. (2014). Happitique's recent setback shows that health app certification is a flawed proposition. *iMedical Apps*. Retrieved from http://www.imedicalapps.com/2014/01/happtiques-setback-future-app-certification/

Nissenbaum, H. F. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford Law Books.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100-126.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296-303. doi:10.1016/j.chb.2014.05.041

Rainie, L, & Duggan, M. (2016). Privacy and Information Sharing. *Pew Research Center*. Retrieved from: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). *Leakiness and creepiness in app space: Perceptions of privacy and mobile app use.* Paper presented at the Proceedings of the 32nd annual ACM conference on Human factors in computing systems.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisclipinary review. *Mis Quarterly, 35*(4), 980-A927.

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, amiajnl-2013-002605.

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empiracle assessment from a field experiment on smartphone users. *Mis Quarterly, 37*(4), 1141.

Wildemuth, B. M. (2009). Applications of social research methods to questions in information and library science. Westport, Conn.: Libraries Unlimited.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). *Measuring mobile users' concerns for information privacy.* Paper presented at the Proceedings of the 33rd International Conference on Information Systems.